

UNITED STATES DISTRICT COURT

for the

Northern District of New York

UNITED STATES OF AMERICA)

v.)

Case No. 3:18-mj-720 (TWD)

JUSTIN HOBBIE)

Defendant)

CRIMINAL COMPLAINT


I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of June 2018 through November 2018 in the county of Otsego in the Northern District of New York the defendant violated:

Code Section
18 U.S.C. § 2252A(a)(2)(A)

Offense Description
Distribution and Receipt of Child Pornography

This criminal complaint is based on these facts:
See attachment

☒ Continued on the attached sheet.



Complainant's signature

James Hamilton, SA HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: Dec 7, 2018


Judge's signature

City and State: Syracuse, NY

Hon. Thérèse Wiley Dancks, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Special Agent James Hamilton of United States Department of Homeland Security, Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the US Immigration and Customs Enforcement Office of Homeland Security Investigations ("HSI") and have been since June 2002. As such, I am an investigative or law enforcement officer of the United States within the meaning of Title 18 United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1). I have been a law enforcement officer for 21 years. I was a police officer for approximately 5 years and have been a Special Agent for 16 years. My career as a Special Agent began in June 2002 with the U.S. Customs Service, which is now known as U.S. Immigration and Customs Enforcement Homeland Security Investigations (HSI). Prior to my employment as a Special Agent, I was a police officer in the state of Tennessee from September 1997 until June 2002. As an HSI Special Agent, I am authorized to seek and execute federal arrest and search warrants for Title 18 criminal offenses, including offenses related to the sexual exploitation of minors, specifically those involving the possession, distribution, and receipt of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have a Bachelor's of Science Criminal Justice degree and a Masters of Public Management degree. I have completed the Criminal Investigator Training Program and Customs Basic Enforcement School at the Federal Law Enforcement Training Center in Glynco, GA. During both basic training, and subsequent training, I received instruction on conducting online child pornography investigations. I have also been the affiant for and participated in the execution of numerous

Federal search warrants in child pornography and child exploitation investigations and have been the affiant of criminal complaints that stem from these investigations.

2. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations and to make arrests for Title 18 offenses enumerated in Section 2516 of Title 18, United States Code.

3. This affidavit is made in support of a criminal complaint charging JUSTIN HOBBIE with violating Title 18, United States Code, Section 2252A(a)(2), Distribution and Receipt of Child Pornography.

4. The statements in this affidavit are based in part on my investigation of this matter, including information that has been told to me by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of supporting a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that JUSTIN HOBBIE has committed the crime of Distribution and Receipt of Child Pornography, in violation of Title 18, United States Code, Section 2252A(a)(2).

BACKGROUND OF THE INVESTIGATION

5. I am assigned to the Internet Crimes Against Children Task Force at the New York State Police in Albany, New York. The ICAC is a task force that partners local, state, and federal law enforcement to investigate crimes involving child exploitation and child pornography. I maintain a covert computer at the ICAC that utilizes a law enforcement version of eMule software that operates on the eDonkey and Kad networks, allowing me to conduct Peer to Peer (P2P)

investigations. My investigative software identifies users of the network that are offering for sharing, files that are suspected child pornography based on the hash values of those files. When a user is identified that is sharing suspected child pornography, my computer will then attempt to directly connect to the IP address offering the suspected child pornography, to download those files from the suspect IP address. Unlike the commercial version of the eMule software which will obtain parts of the file from various sources, the law enforcement version downloads from a single source, that is, only from the IP address offering the suspected child pornography files. For that reason, if the internet connection is interrupted, or the connection with the device at the suspect IP address is lost, I may only receive a partial download, or no download at all. If the connection remains, I often will receive a complete download of the suspected child pornography file from the device that is offering the file at the suspect IP address.

6. On Monday June 18, 2018, my covert computer which was operating the law enforcement version of eMule on the eDonkey network, was directed to a device at IP address 69.207.194.244 because it was associated on the network with one or more files of investigative interest related to child pornography investigations. A direct connection was made to the device at IP address 69.207.194.244, hereinafter referred to as the Suspect Device. The Suspect Device reported that it was using eDonkey client software eMule v0.50a and its client user hash was DB1EA441F60E0BE410A0F64BFB636FFF. Between June 18, 2018 and September 26, 2018, 13 files were downloaded from the Suspect Device to my covert computer through a single source connection. I reviewed the downloaded files and determined that most of the downloaded files contained child pornography. A description of five of the files that were downloaded are as follows:

- a. **46650FE6D55ED410950D9D597D865.mp4**, downloaded 6/18/2018 at 23:26:59 EDT (GMT-4): This file is a 37 second video file depicting a prepubescent girl who appears to be approximately 3-8 years old. The child is naked from the waist down and is wearing a tie-die multi colored t-shirt. In the video, her vagina is exposed to the camera. An adult male's penis is observed being rubbed on the girl's vagina before the tip of the penis is briefly inserted into the girl's anus. The remainder of the video shows the penis being rubbed on the naked anus and vagina of the girl.
- b. **A6AD33BC3FE7CE43919BF03D8B73456D.wmv**, downloaded 6/21/2018 at 23:49:44 EDT (GMT-4): This file is a 20 minute 41 second video file depicting a prepubescent girl, approximately aged 10-12. The video begins showing the girl wearing a red t-shirt and gray pants while sitting in the back of a motor vehicle. She proceeds to take off her clothes, and she picks up a large plastic penis. She rubs the penis on her body, including on her naked vagina. In the video, she also dips the plastic penis into a liquid that appears to be yogurt, and she proceeds to lick the liquid from the penis while she is naked.
- c. **E7C9DC13152009B75FBC08627B059F91.mpg**, downloaded 9/3/2018 at 23:23:17 EDT (GMT-4): This file is a 5 minute 43 second video file that depicts two prepubescent naked children, one boy and one girl, engaged in sexual intercourse. The boy appears to be 9-11 years old, and the girl appears to be 8-10 years old. At the 28 second mark, the children are depicted engaging in sexual intercourse. A third person, an adult male, places his penis inside the girl's mouth.

d. **0FC0A6C358E40796DBA7DB0496247EE8.avi**, downloaded 9/3/2018 at 23:11:11 EDT (GMT-4) and 9/25/2018 at 23:52:52 EDT (GMT-4): This file is a 6 minute 36 second video depicting a prepubescent girl, approximately age 9-11. A watermark on the bottom right corner of the screen states “vichatter.net” indicating this is a recorded video chat session. A blonde-haired girl wearing a multi-colored dress appears to be sitting in front of a computer monitor while communicating with another person. At the 4 minute 38 second mark, she steps back from the computer, and lifts her dress exposing her naked vagina to the camera. At the 6 minute 19 second mark, she stands on the chair in front of the computer, and lifts one leg into the air, exposing her vagina and anal regions to the person she is communicating with.

e. **4662EE6029281C9EAE33655B1F48ABA2.avi**, downloaded 9/20/2018 at 23:31:29 EDT (GMT-4) and 9/26/2018 at 00:34:56 EDT (GMT-4): This file is a 2 minute 6 second video file depicting a prepubescent girl who appears to be approximately 8-12 years old. She begins the video wearing a purple t-shirt and shorts or pants, and then she is naked by the middle of the video. The girl sits naked in a chair, with her knees drawn to her chest, exposing her vagina to the camera as she rubs her vagina with her fingers. While she rubs her vagina with her fingers, at the 1 minute 38 second mark, a naked adult male enters the video screen. The male places his naked penis into the girl’s mouth.

7. My law enforcement software identified that IP address 69.207.194.244 belongs to Time Warner Cable, an internet service provider that has been merged with Charter

Communications. I verified this IP address as a Time Warner Cable address using an open source website on the internet.

8. On November 5, 2018, I served a Department of Homeland Security Form 3115 administrative summons to Time Warner Cable d/b/a Charter Communications requesting subscriber information for IP address 69.207.194.244 for the dates that the downloads were made from the Suspect Device to my computer. I also asked for the service start and end dates for IP address 69.207.194.244. On November 7, 2018, Charter Communications responded that the IP address 69.207.194.244 was assigned to customer Justin HOBBIE with a physical address in Springfield Center, New York (the Subject Premises) and a billing address in Springfield Center, New York. Further, the response also stated that the IP address 69.207.194.244 was assigned to HOBBIE at the Subject Premises from September 3, 2017 through October 3, 2018, which encompasses all of the dates and times of the above listed files that were downloaded from HOBBIE's IP address to my law enforcement computer.

9. On November 14, 2018, I queried the New York State Department of Motor Vehicles database and found that Justin HOBBIE, DOB XX/XX/1977, has a valid driver's license listing an address in Springfield Center, New York 13468.

10. On November 19, 2018, I served a second Department of Homeland Security Form 3115 administrative summons to Time Warner Cable d/b/a Charter Communications requesting subscriber information for IP address 69.207.194.244 for the specific dates and times of the downloaded child pornography files that are described above in paragraphs 6a- 6e. On the same date, Charter Communications responded that IP address 69.207.194.244, on the dates and times the child pornography files listed in paragraphs 6a – 6e were downloaded from the Suspect Device

to my covert computer, was assigned to customer Justin HOBBIIE with a physical address in Springfield Center, New York (the Subject Premises).

11. On November 19, 2018, at approximately 9:30 AM, I drove by the Subject Premises several times to conduct a check for open Wi-Fi internet connections. In front of the SUBJECT PREMISES there was a "Spectrum" Wi-Fi signal that was secured. Spectrum is a name of the company operating because of the merger of Time Warner Cable and Charter Communications, although the Time Warner Cable and Charter Communications names are still in use. Other Wi-Fi signals near the SUBJECT PREMISES were secure.

12. On November 19, 2018, while checking my covert computer for downloads in my eMule software, I discovered that my computer had downloaded several files from IP address 67.242.108.249 on November 9, 2018 through November 12, 2018. My interest in these downloads was piqued because geographically, it resolves to Cooperstown, New York, the area the original IP address associated with this investigation geo locates to. Furthermore, I discovered that the downloads from IP address 67.242.108.249 came from Client User Hash DB1EA441F60E0BE410A0F64BFB636FFF. This is the same Client User Hash in which the downloads from IP address 69.207.194.244, from which the files listed in paragraph 6a – 6e were downloaded. The Client User Hash is a unique identifier assigned to each individual computer or electronic device that is operating on the eDonkey network. Also, the Suspect Device reported that it was using eDonkey client software eMule v0.50a, the same version of software that the Suspect Device was using during the downloads between June 18, 2018 and September 26, 2018. During the November 9 – 12, 2018 time frame, 8 files were downloaded from the Suspect Device at IP address 67.242.108.249 to my covert computer through a single source connection. I reviewed

the downloaded files and determined that most of the downloaded files contained child pornography. A description of three of the files are as follows:

- a. **46650FE6D55ED410950D9D597D865.mp4**, downloaded 11/10/2018 at 00:02:50 EST (GMT-5): This file is a 37 second video file depicting a prepubescent girl who appears to be approximately 3-8 years old. The child is naked from the waist down and is wearing a tie-die multi colored t-shirt. In the video, her vagina is exposed to the camera. An adult male's penis is observed being rubbed on the girl's vagina before the tip of the penis is briefly inserted into the girl's anus. The remainder of the video shows the penis being rubbed on the naked anus and vagina of the girl.
- b. **013D6520AAD370BA92C9272DE656F7EC.wmv**, downloaded 11/10/2018 at 00:21:00 EST (GMT-5): This file is a 12 minute 56 second video file depicting a prepubescent girl who appears to be approximately 7-10 years old. She is naked except for a mask on her face. Also, in the video is a naked adult male, who is wearing a clown mask. In the video, the male subjects the child to various sexual acts, including placing his hand inside her vagina; placing his penis inside her mouth, sexual intercourse, and placing a plastic object inside her vagina.
- c. **5E106176EA00247509427A47099154E8.mpg**, downloaded 11/12/2018 at 00:14:02 EST (GMT-5): This file is a 11 minute 42 second video file depicting a prepubescent girl, approximately 7-10 years old. She is naked except for stockings that she is wearing on her legs. The video depicts a naked adult male rubbing his penis on her vagina. Later he places his penis into her mouth. Near the end of the video, the adult male masturbates with his penis in front of the girl's face.

13. On November 20, 2018, I served a third Department of Homeland Security Form 3115 administrative summons to Time Warner Cable d/b/a Charter Communications. This summons requested subscriber information for IP address 67.242.108.249 for the dates and times of the video files described in paragraphs 18a - 18c. On the same date, Charter Communications responded that on all of the dates and times requested, which include the dates and times listed in paragraphs 18a - 18c, IP address 67.242.108.249 was assigned to Justin HOBBIE at the Subject Premises. Additionally, the response states that the IP address assignment to HOBBIE's account began on October 2, 2018 and continues into November 21, 2018.

14. On November 25, 2018, at approximately 11:10 PM, I conducted a brief surveillance of the Subject Premises. During the surveillance, I observed that the residence was dark except for a light in the basement at the end of the house opposite the front entrance, and a light in a room located at the rear of the house, between the house and the garage/driveway area. I conducted a second check for secured Wi-Fi internet during this surveillance. While standing on the road in front of the Subject Premises, I found that there were 5 Wi-Fi internet access points available. All 5 connections were secured.

15. Based on my investigation, experience, and the facts established in the above paragraphs, probable cause was established to show that an electronic device, while connected to the internet at the Subject Premises, did possess and distribute child pornography in violation of 18 U.S.C. §§ 2252 and 2252A. A federal search warrant was issued on November 29, 2018, by the United States District Court for the Northern District of New York to search the Subject Premises, Justin HOBBIE, his vehicles, and any computers, and electronic devices, and electronic storage media that are located during the course of the search.

EXECUTION OF FEDERAL SEARCH WARRANT

16. On December 6, 2018, your affiant, along with other HSI special agents and New York State Police investigators executed a search warrant at the Subject Premises that was authorized by this Court on November 29, 2018.

17. Justin HOBBIE was present at the residence when agents arrived. HOBBIE agreed to go to the nearby New York State Police barracks in Richfield Springs, New York for an interview with your affiant and Special Agent Justin Jones. At the New York State Police barracks, HOBBIE was read his *Miranda* warning. HOBBIE waived his *Miranda* rights in writing and agreed to speak with your affiant and Special Agent Jones.

18. During the course of the interview HOBBIE stated that the Alienware gaming computer located in his basement was purchased new in approximately 2010. HOBBIE stated that he uses the computer for gaming, and graduate school studies. He further stated that several years ago, he installed eMule and Bit Torrent Peer to Peer (P2P) filesharing programs on the computer. He stated that at one time he used the search word “teen” on his eMule P2P program and received child pornography files, including a child pornography video file that he described as featuring a 8 or 9 year old girl. The computer was password protected and Hobbie provided the password for the computer. An interview of the subject’s wife which was conducted simultaneously revealed that Justin Hobbie is the sole user of the Alienware computer. His wife also stated that approximately 13 years ago she discovered child pornography on a computer Hobbie was using and confronted him about it and made him delete the child pornography from that computer. When questioned about this incident Hobbie admitted that child pornography was found by his wife on a previous computer but claimed not to know how it got on the computer.

19. While at HOBBIIE's residence during the execution of the search warrant, New York State Police Computer Crimes Investigator Mathew Burkert conducted a field forensic preview of HOBBIIE's Alienware computer that was found in the basement of the residence. That preview revealed an elaborate file folder system that HOBBIIE used to store and categorize the child pornography he downloaded. Within those files Investigator Burkett found at least 50 images and 50 videos containing child pornography. Among those files Investigator Burkert found the following video files that had been saved on the computer in the "download folder" file path:

- a. **Lsm02-05-01.mpg-** Filepath: c:\users\admin\downloads\ls studio\enjoy the show\issue 02 enjoy the show\videos\lsm02-05-01.mpg. This 7 minute 36 second video depicts two girls, approximately age 10-12 years old, that begin the video dressed in skirts and shirts. The video ends with the girls naked, dancing, and touching each other, with the camera focused closely on the naked vaginal areas of the girls. The file was saved into the folder on the computer on November 7, 2018.
- b. **Lsm14-01-02.mpg-** Filepath: c:\users\admin\downloads\ls studio\everything_about_me\i_14_everything_about_me\videos\lsm14-01-02.mpg. This 6 minute 54 second video begins with two girls, approximately aged 6-8 years old, lying naked on a bed together. The camera focusses closely on the vaginal areas of both girls. The girls begin to pillow fight in the video. The video ends with both girls pretending to be asleep, one girl has the blanket pulled away from her exposing her vaginal area to the camera. The file was saved into the folder on the computer on November 7, 2018..
- c. **Lsm14-01-03.mpg** Filepath: c:\users\admin\downloads\ls studio\everything_about_me\i_14_everything_about_me\videos\lsm14-01-

03.mpg. This 2 minute 54 second video depicts two naked girls, approximately 8-10 years old. One girl is laying naked on a table, with a bowl of food on her chest. The other girl, standing next to the table, rubs food product on the other girl's body. The camera focusses closely on the vaginal areas of both girls. The file was saved into the folder on the computer on November 7, 2018.

- d. **Lsm14-03-01.mpg** Filepath: c:\users\admin\downloads\ls
studio\everything_about_me\i_14_everything_about_me\videos\lsm14-03-
01.mpg. This 5 minute 15 second video begins with two naked girls, approximately aged 6-8 years old, bending over, dancing their bodies in a manner that focuses on the viewer seeing their vaginal areas. The girls have drawings on their bodies. The video ends with the girls drawing shapes and pictures on each other's bodies using markers, while the camera focuses on their naked vaginal areas. The file was saved into the folder on the computer on November 7, 2018.

20. During my investigation of Justin HOBBIE's IP address prior to the execution of the search warrant on December 6, 2018, my covert computer had downloaded several files from IP address 67.242.108.249 on November 9, 2018 through November 12, 2018. This IP address is assigned to Justin HOBBIE's residence by Time Warner Cable/Charter Communications. The downloads from IP address 67.242.108.249 came from a device operating an eMule program with Client User Hash DB1EA441F60E0BE410A0F64BFB636FFF. The Client User Hash is a unique identifier assigned to each individual computer or electronic device that is operating on the eDonkey network. Also, the Suspect Device reported that it was using eDonkey client software eMule v0.50a. During the November 9 – 12, 2018 time frame, 8 files were downloaded from the Suspect Device at IP address 67.242.108.249 to my covert computer through a single source

connection. I reviewed the downloaded files and determined that most of the downloaded files contain child pornography. A description of three of the files are as follows:

- a. **46650FE6D55ED410950D9D597D865.mp4**, downloaded 11/10/2018 at 00:02:50 EST (GMT-5): This file is a 37 second video file depicting a prepubescent girl who appears to be approximately 3-8 years old. The child is naked from the waist down and is wearing a tie-die multi colored t-shirt. In the video, her vagina is exposed to the camera. An adult male's penis is observed being rubbed on the girl's vagina before the tip of the penis is briefly inserted into the girl's anus. The remainder of the video shows the penis being rubbed on the naked anus and vagina of the girl.
- b. **013D6520AAD370BA92C9272DE656F7EC.wmv**, downloaded 11/10/2018 at 00:21:00 EST (GMT-5): This file is a 12 minute 56 second video file depicting a prepubescent girl who appears to be approximately 7-10 years old. She is naked except for a mask on her face. Also, in the video is a naked adult male, who is wearing a clown mask. In the video, the male subjects the child to various sexual acts, including placing his hand inside her vagina, placing his penis inside her mouth, sexual intercourse, and placing a plastic object inside her vagina.
- c. **5E106176EA00247509427A47099154E8.mpg**, downloaded 11/12/2018 at 00:14:02 EST (GMT-5): This file is a 11 minute 42 second video file depicting a prepubescent girl, approximately 7-10 years old. She is naked except for stockings that she is wearing on her legs. The video depicts a naked adult male rubbing his penis on her vagina. Later he places his penis into her mouth. Near the end of the video, the adult male masturbates with his penis in front of the girl's face.


21. The videos described in paragraphs 20 a-c were distributed from a computer or device using Justin HOBBIE's assigned IP address as described in paragraph 20. During the execution of the search warrant at HOBBIE's residence, while Investigator Burkert was conducting a field preview of HOBBIE's Alienware computer located in the basement of his residence, Investigator Burkert discovered that the computer has an eMule client hash of DB1EA441F60E0BE410A0f64BFB636FFF. Investigator Burkert found that the client hash was located in the file c:\Users\Admin\AppData\Local\eMule\config\preferences.dat. Of significance is that this client hash is the same client hash for the device that the child pornography video files were downloaded from when my covert computer downloaded the files from Justin HOBBIE's assigned IP address. In other words, this analysis shows that my covert computer downloaded the files from the Alienware computer that was seized from Justin HOBBIE's basement during the execution of the search warrant.

22. The images referenced above are available for the Court's review upon request.

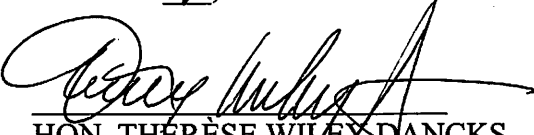
23. In addition to the child pornography files found on Hobbie's Alienware computer forensic investigators also found a child pornography video located on Hobbie's Samsung personal cellular telephone. That video depicts a snapchat session with a minor who can be seen penetrating her vagina with a dildo.

CONCLUSION

24. Based on the foregoing information, there is probable cause to conclude that JUSTIN HOBBIE did knowingly receive and distribute child pornography using a means and facility of interstate and foreign commerce, and in and affecting such commerce, that is, through downloading and sharing video files depicting child pornography over the internet using the e-Mule file sharing application, in violation of Title 18, United States Code, Section 2252A(a)(2)(A).


Special Agent James Hamilton
Homeland Security Investigations

Subscribed and sworn to before me on
December 7, 2018


HON. THERÈSE WILEY DANCKS
United States Magistrate Judge